IN THE CLAIMS

1. (Currently Amended) A method, comprising the steps of:

defining a plurality of records;

qualifying an access to a record by referencing a respective set of access rules for the record, said respective access rules being stored in a database representing respective sets of access rules for said plurality of records, and said respective set of access rules comprising instructions to a trustee, defined under a legally enforceable trust agreement establishing a trust granting legal control over access to the record to a trustee subject to jurisdictional law of trusts, on behalf of a beneficiary;

receiving a third party public key having an associated third party private key, and defining a session key for communication of a record; ~~and~~

applying the respective set of access rules, retrieved from the database, to selectively grant access to the record by a third party, by means of an automated system, wherein said automated system provides a communication of the record in an encrypted form associated with a logging wrapper, wherein the record is cryptographically protected with both the third party public key and the session key, the limitations of the trust being enforced under authority of the trustee in accordance with the trust agreement, the respective set of access rules, and the jurisdictional law of trusts,

wherein access to a decrypted content of the record requires decryption of the communication with respect to the session key, and supply of the third party private key, and said logging wrapper generates a logging event, and

recording the logging event in an access log.

2. (Previously Presented) The method according to claim 1, wherein the record is encrypted, further comprising the step of accounting for a decryption of the record after access to at least a portion thereof.

3. (Original) The method according to claim 2, wherein said accounting is anonymous.

4. (Previously Presented) The method according to claim 1, wherein the record has a plurality of portions, at least one portion being encrypted with at least one cryptographic key, said portions being independently accessible, said respective set of access rules applying to selectively limit access to portions of the record.

5. (Previously Presented) The method according to claim 4, wherein said respective set of access rules limit access to portions based on an identity of an intended recipient.

6. (Previously Presented) The method according to claim 1, further comprising the step of supplying a decryption key for a respective record portion in accordance with the respective set of access set of rules.

7. (Previously Presented) The method according to claim 1, further comprising the step of accounting for attempted access to at least a portion of the record.

8. (Previously Presented) The method according to claim 1, wherein the respective set of access rules are associated with an intended recipient of the record.

9. (Original) The method according to claim 1, further comprising the step of referencing an index to define a record.

10. (Original) The method according to claim 9, wherein the index further stores a set of access rules for qualifying an intended recipient with respect to each of the records.

11. (Original) The method according to claim 1, further comprising the step of using an index to identify a record potentially responsive to a query.

12. (Original) The method according to claim 1, further comprising the step of using an index comprising a set of associations of patient identities and medical transaction records to identify records relating to a respective patient.

13. (Original) The method according to claim 1, further comprising the step of using an index comprising a set of associations of record identification, record characteristic, and said access rules to identify records relating to a query and limiting access to portions thereof.

14. (Original) The method according to claim 1, wherein the record comprises a plurality of portions, the portions being separately encrypted and having associated sets of independent rules.

15. (Original) The method according to claim 1, wherein the access rules are role based access rules relating to a role of the intended recipient.

16. (Original) The method according to claim 1, wherein the access rules are context based access rules relating to a context of record access.

17. (Previously Presented) The method according to claim 1, wherein the respective set of access rules are defined by a grantor of the trust.

18. (Previously Presented) The method according to claim 1, wherein the record is encrypted, and a decryption of the record triggers a remotely-sensed transaction.

19. (Original) The method according to claim 18, wherein the remotely sensed transaction comprises a financial accounting transaction.

20. (Original) The method according to claim 18, wherein the remotely sensed transaction comprises an access audit trail transaction.

21. (Original) The method according to claim 2, wherein said accounting occurs upon supply of the respective decryption key.

22. (Original) The method according to claim 2, wherein said accounting occurs upon use of the respective decryption key.

23. (Original) The method according to claim 1, wherein the record comprises a medical record.

24. (Original) The method according to claim 1, wherein the record comprises a media content record.

25. (Previously Presented) The method according to claim 1, wherein the access rules are interpreted in accordance with a database of jurisdictional trust laws.

26. (Previously Presented) The method according to claim 1, wherein the respective set of access rules are interpreted in accordance with a database of jurisdiction-dependent privacy laws.

27. (Previously Presented) The method according to claim 1, further comprising the step of creating a trust comprising the record, implemented in accordance with the trust laws of a specified jurisdiction.

28. (Previously Presented) The method according to claim 1, wherein the record comprises separate articles within a digital publication.

29. (Previously Presented) The method according to claim 1, further comprising the step of receiving the respective set of access rules.

30. (Previously Presented) The method according to claim 1, further comprising the step of generating the respective set of access rules based on the record.

31. (Previously Presented) The method according to claim 1, wherein the record is encrypted with an encryption scheme having a rolling code.

32. (Previously Presented) The method according to claim 1, wherein the trustee controls the records and implements the access rules without requiring access to a content of the records.

33. (Previously Presented) The method according to claim 1, wherein the trustee acts without requiring access to the records.

34. (Original) The method according to claim 1, wherein the trustee selectively processes the records.

35. (Original) The method according to claim 1, wherein the records comprise a type selected from the group consisting of legal information, government records, financial records, commercially valuable trade secret legal information, manufacturing information, banking information, consumer entertainment media, digital music files, video information, cinema information, consumer information, personal demographic information, credit card

information, personal contact information, social security number information, publication information, separate articles within a digital publication, and investment account information.

36. (Previously Presented) The method according to claim 1, wherein the record comprises a patient file, placed in a privileged trust for the patient with a trustee, said trustee implementing the respective set of access rules with respect to each transaction record within the patient file defined by the patient and legal jurisdiction, wherein said trustee interacts with the patient record information to at least one of maintain, process, receive, deliver, and transmit portions of the patient file in secure and verifiable fashion to authorized entities in compliance with the trust.

37. (Previously Presented) The method according to claim 1, wherein the record comprises a corpus of a medical information trust for holding medical records on behalf of a patient distinct from the caregiver; the trustee charging for access to the medical record, and maintaining a record of each access of the medical record.

38. (Previously Presented) The method according to claim 1, wherein the trust has a beneficiary and the respective set of access rules is applied to limit access by an identified intended recipient, without communicating an identity of the intended recipient to the beneficiary.

39. (Previously Presented) The method according to claim 1, further comprising the steps of:

placing information represented by the record in legal trust under control of a trustee on behalf of the beneficiary, said information being stored in electronically readable form;

automatically authorizing access to the information in trust based on compliance with a trust-defined rule, comprising requiring an electronic communication between a user and the trustee; and

permitting an authorized user to access the information in the trust through an electronic communication.

40. (Previously Presented) The method according to claim 39, wherein the trust defined rule comprises a compensation rule for obtaining a right to the information.

41. (Original) The method according to claim 40, wherein the electronic communication comprises an electronic funds transfer.

42. (Original) The method according to claim 40, wherein the compensation rule is integrally associated with the information, and wherein the implementing occurs as a result of user interaction with the information.

43. (Original) The method according to claim 39, wherein the information comprises a patient medical record.

44. (Original) The method according to claim 39, wherein the information comprises consumer entertainment media.

45. (Previously Presented) The method according to claim 39, wherein the trustee is interposed between the beneficiary and the user, the trustee maintaining an anonymity of the user while accounting to the beneficiary.

46. (Previously Presented) The method according to claim 39, wherein the trustee is interposed between the beneficiary and the user, the trustee characterizing the user based on a classification of information usage, while accounting to the beneficiary for the use, without specifically identifying information usage of a user.

47. (Previously Presented) The method according to claim 39, wherein a transfer of the information to the user requires an electronic transfer of value from the user to the trustee, further comprising the step of accepting the value by the trustee while stripping an identification of the user from a retained transfer record.

48. (Original) The method according to claim 39, further comprising the steps of receiving an identification of desired information content from a user; and logging the access employing a digital signature of the user.

49. (Original) The method according to claim 48, wherein the digital signature is anonymous with respect to the beneficiary.

50. (Previously Presented) The method according to claim 48, wherein the authorizing step entails requiring the user to enter into a restrictive covenant.

51. (Previously Presented) The method according to claim 40, wherein the trustee manages access to the information and implements the respective set of access rules as an intermediary for, and communicates compensation information to, the beneficiary.

52. (Previously Presented) The method according to claim 40, wherein the information has an associated compensation value, and comprises digital media information, said digital media information being associated with subsidy content having an associated subsidy value, further comprising the step of accounting for use of the digital media information offset by the subsidy value.

53. (Previously Presented) The method according to claim 1, further comprising the steps of:

defining information content of a record and an associated set of access rules;

electronically transmitting the information content and associated set of access rules to the trustee subject to the terms of the trust agreement;

storing the transmitted information content and associated set of access rules as a respective one of the plurality of records and a respective set of access rules; and

automatically implementing, under control of the trustee, the associated access rules with respect to the information content, to establish a virtual trust in accordance therewith, whereby the trustee selectively authorizes access to the information content to selectively permit communication of the information content.

54. (Original) The method according to claim 53, wherein the information content comprises media information, and the associated access rules comprise economic rules.

55. (Original) The method according to claim 53, wherein the information content comprises medical record information, and the associated access rules comprise restrictive access rules based on an identity or characteristic of the user.

56. (Original) The method according to claim 55, further comprising the step of transmitting, from the trustee, information content in accordance with the associated rules.

57. (Original) The method according to claim 53, wherein the trustee controls the information content and implements the rules without requiring access to the information content.

58. (Currently Amended) A database system, comprising a plurality of records, each record having an associated set of access rules, means for automatically applying the appropriate set of access rules to control access to the record by a third party, each respective set of access rules representing instructions to a trustee operating under an established legal trust applying the access rules on behalf of a beneficiary in accordance with the legal trust, the respective access rules, and the jurisdictional trust law, wherein the record is communicated in an encrypted form requiring for decryption at least a session key and a private key of a public key-private key pair, and wherein access of the record is controlled through a wrapper which is adapted to generate an access event in an access log.

59. (Previously Presented) The system according to claim 58, wherein the record is encrypted, further comprising means for accounting for a decryption of the record.

60. (Original) The system according to claim 59, wherein said accounting is anonymous.

61. (Previously Presented) The system according to claim 58, wherein the record has a plurality of portions, each portion being encrypted with at least one cryptographic key, said portions being independently accessible, said respective access rules applying to selectively limit access to portions of the record.

62. (Original) The system according to claim 61, wherein said access rules limit access to portions based on an identity of an intended recipient.

63. (Previously Presented) The system according to claim 58, wherein the record comprises a plurality of encrypted portions, further comprising the step of supplying a decryption key for a respective record portion in accordance with the respective access rules.

64. (Previously Presented) The system according to claim 58, wherein at least a portion of the record is encrypted, further comprising an accounting system for accounting for a decryption of a portion of the record.

65. (Previously Presented) The system according to claim 58, wherein the respective access rules are associated with an intended recipient of the record.

66. (Original) The system according to claim 58, further comprising the step of referencing an index to define a record.

67. (Previously Presented) The system according to claim 66, wherein the index further stores respective access rules for qualifying an intended recipient with respect to each of the records.

68. (Original) The system according to claim 67, further comprising the step of using an index to identify a record potentially responsive to a query.

69. (Previously Presented) The system according to claim 58, wherein the record comprises a medical record, and wherein an index of a set of associations of patient identities and medical transaction records is used to identify records relating to a respective patient.

70. (Previously Presented) The system according to claim 58, wherein an index of a set of associations of record identification, record characteristic, and said respective access rules to identify records relating to a query and limiting access to portions thereof.

71. (Previously Presented) The system according to claim 58, wherein the record comprises a plurality of portions, the portions being separately encrypted and having associated therewith sets of independent respective rules.

72. (Previously Presented) The system according to claim 58, wherein the respective access rules are role based access rules relating to a role of an intended recipient.

73. (Previously Presented) The system according to claim 58, wherein the respective access rules are context based access rules relating to a context of record access.

74. (Previously Presented) The system according to claim 58, wherein the respective access rules are defined by a grantor of the trust.

75. (Original) The system according to claim 58, wherein a decryption of the record triggers a remotely-sensed transaction.

76. (Original) The system according to claim 75, wherein the remotely sensed transaction comprises a financial accounting transaction.

77. (Original) The system according to claim 75, wherein the remotely sensed transaction comprises an access audit trail transaction.

78. (Original) The system according to claim 59, wherein said accounting occurs upon supply of the respective decryption key.

79. (Original) The system according to claim 59, wherein said accounting occurs upon use of the respective decryption key.

80. (Original) The system according to claim 58, wherein the record comprises a medical record.

81. (Original) The system according to claim 58, wherein the record comprises a media content record.

82. (Previously Presented) The system according to claim 58, wherein the respective access rules are interpreted in accordance with a database of jurisdictional trust laws.

83. (Previously Presented) The system according to claim 58, wherein the respective access rules are interpreted in accordance with a database of jurisdiction-dependent privacy laws.

84. (Original) The system according to claim 58, further comprising the step of creating a virtual trust encompassing the record, implemented in accordance with the trust laws of an associated jurisdiction.

85. (Original) The system according to claim 58, wherein the records comprise separate articles within a digital publication.

86. (Previously Presented) The system according to claim 58, further comprising the step of receiving the respective access rules.

87. (Previously Presented) The system according to claim 58, further comprising the step of generating the respective access rules based on the record.

88. (Previously Presented) The system according to claim 58, wherein a record is encrypted with an encryption scheme having a rolling code.

89. (Previously Presented) The system according to claim 58, wherein the trustee controls the records and implements the respective access rules without requiring access to a content of the record.

90. (Original) The system according to claim 58, wherein the trustee controls access to the records.

91. (Original) The system according to claim 58, wherein the trustee selectively processes the records.

92. (Original) The system according to claim 58, wherein the records comprise a type selected from the group consisting of legal information, government records, financial records, commercially valuable trade secret legal information, manufacturing information, banking information, consumer entertainment media, digital music files, video information, cinema information, consumer information, personal demographic information, credit card information, personal contact information, social security number information, publication information, separate articles within a digital publication, and investment account information.

93. (Previously Presented) The system according to claim 58, wherein a record comprises a patient file, placed in a privileged trust for the patient with a trustee, said trustee implementing the set of rules for access with respect to each transaction record within the patient file, the respective rules being defined by the patient and legal jurisdiction, wherein said trustee interacts with the patient record information to at least one of maintain, process, receive, deliver,

and transmit portions of the patient record in secure and verifiable fashion to authorized entities in compliance with the trust.

94. (Cancelled).

95. (Cancelled).

96. (Cancelled).

97. (Cancelled).

98. (Cancelled).

99. (Cancelled).

100. (Cancelled).

101. (Cancelled).

102. (Cancelled).

103. (Cancelled).

104. (Cancelled).

105. (Currently Amended) The ~~system~~ method according to claim 58 ~~96~~, ~~further comprising means for receiving an identification of desired information content from a user; and means for logging the access employing~~ wherein the wrapper logs the access based on a digital signature of the third party ~~user~~.

106. (Currently Amended) The ~~system~~ method according to claim 1 ~~105~~, wherein the logging wrapper logs the access based on a digital signature of the third party ~~is anonymous with respect to the beneficiary~~.

107. (Currently Amended) The ~~system~~ method according to claim 1 ~~96~~, wherein the ~~user~~ third party is required to enter into a restrictive covenant for access to the information.

108. (Cancelled).

109. (Currently Amended) The system according to claim 58 ~~97~~, wherein the information ~~has an associated compensation value, and~~ comprises digital media information, said digital media information being associated with subsidy content, wherein an economic compensation for access by the ~~user~~ third party to ~~accounts to said selective access providing means for use of~~ the digital media information is offset by a value for subsidy content.

110. (Previously Presented) The database system according to claim 58, further comprising:

a set of associated selective rights, corresponding to a record, held as at least a portion of a corpus of a trust, for restricting at least one of access, use, storage and transmission of a respective set of defined content information, organized as a legal entity under the laws of a jurisdiction; and

a trustee acting under the trust laws of the jurisdiction, receiving the associated rights and implementing a virtual trust in accordance therewith,

wherein the trustee communicates through an electronic communications system to selectively convey permission to at least one of access, use, store and transmit the respective set of defined content information in accordance with the respective access rules.

111. (Previously Presented) The system according to claim 110, wherein the information content comprises media information, and the rights comprise economic rules.

112. (Previously Presented) The system according to claim 110, wherein the information content comprises medical record information, and the rights comprise restrictive access rules based on an identity or characteristic of the user.

113. (Previously Presented) The system according to claim 112, further comprising the step of transmitting, from the trustee, information content in accordance with the rights.

114. (Previously Presented) The system according to claim 110, wherein the trustee controls the information content and implements rights-based restrictions without requiring access to the information content.

115. (Original) The system according to claim 110, wherein the defined information content is provided as a set of records, each record having a plurality of portions, at least two such portions being associated with independent cryptographic keys, further comprising a database index providing an association between a record descriptor, a record identification, and a set of limiting access rules for each privileged database record; and a cryptographic key database, for storing cryptographic keys associated with portions of a record.

116. (Previously Presented) The system according to claim 110, wherein said rights are a set of rules selected from the group consisting of one or more of role based access rules, and context based access rules.

117. (Original) The system according to claim 115, wherein each of the portions is encrypted with at least one cryptographic key, said portions being independently accessible.

118. (Original) The system according to claim 115, further comprising means for accounting for a decryption of an encrypted record or portion of a record.

119. (Original) The system according to claim 115, wherein the records comprise medical records.

120. (Previously Presented) The system according to claim 110, wherein the rights are interpreted in accordance with a database of jurisdictional trust laws.

121. (Previously Presented) The system according to claim 110, wherein the rights are jurisdiction-dependent, further comprising an input for receiving an identification of a relevant jurisdiction.

122. (Original) The system according to claim 121, further comprising means for resolving inconsistencies between a plurality of relevant jurisdictions.

123. (Previously Presented) The system according to claim 121, further comprising a plurality of sets of rights, each set of rights being associated with a different jurisdiction, further comprising means for applying a set of rights relevant to an associated jurisdiction.

124. (Previously Presented) The system according to claim 110, further comprising a transaction log including a digital signature of a transactor, wherein the transaction log may be audited through authentication of the digital signature.

125. (Original) The system according to claim 124, wherein the transaction log may be audited without revealing an identity of the transactor.

126. (Original) The system according to claim 124, wherein the transaction log audited reveals an identity of the transactor.

127. (Previously Presented) The method according to claim 1, wherein the record comprises a plurality of medical transaction information files, associated with the specific patient, each medical transaction information file being separately encrypted, and being subject to a separate role-based access rule and a searchable index identifying a content of said medical transaction information files, a search of said index being role-based rule sensitive to withhold index information from unauthorized users.

128. (Previously Presented) The method according to claim 127, wherein the record comprises at least two medical transaction information files, each file being separately encrypted.

129. (Previously Presented) The method according to claim 127, further comprising respective access rule embedded in the medical transaction information file.

130. (Previously Presented) The method according to claim 127, wherein the respective access rule is not encrypted.

131. (Previously Presented) The method according to claim 127, wherein the medical transaction file encryption comprises public key encryption.

132. (Previously Presented) The method according to claim 127, wherein the medical transaction file encryption comprises multiple levels of public key encryption, employing differing keys.

133. (Previously Presented) The method according to claim 127, wherein the medical transaction file encryption comprises a first public key encryption employing a patient-specific public key, and a second public key encryption employing a recipient specific public key.

134. (Previously Presented) The method according to claim 127, wherein the medical transaction file encryption comprises a public key encryption employing a recipient-system interaction specific key.

135. (Previously Presented) The method according to claim 134, wherein the medical transaction file encryption further comprises a first public key encryption employing a patient-specific public key, and a second public key encryption employing a recipient specific public key.

136. (Previously Presented) The method according to claim 134, wherein said recipient-system interaction specific key interacts with an applet wrapper to decrypt the medical record.

137. (Previously Presented) The method according to claim 127, wherein the record is in a database system for hosting the medical transaction information files, further comprising the step of accounting for access to a content of each of said encrypted medical transaction information files.

138. (Previously Presented) The method according to claim 137, wherein the accounting is a financial accounting.

139. (Previously Presented) The method according to claim 137, further comprising the step of generating an audit trail.

140. (Previously Presented) The method according to claim 1, wherein at least one of the respective access rules comprises:

charging for access to or permission to access the record by causing at least one of a monetary transfer through a monetary transfer system and an accounting entry in an accounting database representing a proposed monetary transfer; and

storing a record of at least one of each access of and permission to access the record in a database.

141. (Original) The method according to claim 140, wherein the access permission comprises a cryptographic key.

142. (Previously Presented) The method according to claim 1, further comprising the steps of:

establishing under jurisdictional trust laws, in an entity distinct from a rights holder, a virtual information trust in accordance with the legally enforceable trust agreement, to hold the record or associated access permission on behalf of a beneficiary;

providing a database system, comprising a plurality of records, each record having an associated set of respective access rules;

the trustee operating under the virtual information trust and applying the respective access rules on behalf of the beneficiary in accordance with the virtual information trust;

charging for access to or permission to access the content record by causing at least one of a monetary transfer and an accounting entry representing a proposed monetary transfer; and

maintaining a record of each access of or permission to access the content record.

143. (Original) The method according to claim 142, wherein the access permission comprises a cryptographic key.

144. (Currently Amended) A method, comprising the steps of:

storing a set of access rules in a database;

defining a plurality of sets of information content, the sets of information content being subject to associated access rules stored in the database;

transmitting information defining the associated access rules for the respective plurality of sets of information content to a trustee;

automatically, under control of the trustee, retrieving the associated access rules with respect to the associated information content, and implementing the retrieved associated access rules dependent on a context of attempted access of the associated information content, and in

accordance with a trust agreement under which the trustee has a duty to a beneficiary in accordance with a jurisdictional law of trusts; and

accounting, by the trustee, for access to the information content and respective context in an access log based on a wrapper associated with the information content,

the access to a decrypted form of the information content being dependent at least a session key and a private key of a public key-private key pair.

145. (Previously Presented) The method according to claim 144, wherein the trustee commercially exploits the record.

146. (Previously Presented) The method according to claim 144, wherein the trustee generates commercial subsidies in conjunction with transactions involving a record.

147. (Previously Presented) The method according to claim 144, wherein the trustee conducts a financial transaction with respect to a record, and financially compensates the beneficiary for the transaction.

148. (Previously Presented) The method according to claim 144, further comprising the step of presenting paid advertising to an accessor of the record.

149. (Previously Presented) The method according to claim 144, further comprising the step of presenting context-sensitive advertising to an accessor of the record, paid by the advertiser based on a quantity of presentation thereof.

150. (Previously Presented) The method according to claim 149, wherein an accounting to the advertiser excludes confidential information.

151. (Previously Presented) The method according to claim 1, further comprising the steps of:

(a) defining the terms of a legally enforceable trust between a grantor and a trustee, on behalf of a beneficiary, for maintaining an information record in trust subject to the respective set of access rules, said information record comprising property of value;

(b) conveying the information record to the trustee, as a corpus of the trust; and

(c) accounting to the beneficiary for financial value attributable to the trust.

152. (New) A database system, comprising:

at least one retrieval subsystem adapted to retrieve a plurality of records and having at least one access log, each record having an associated set of access rules;

at least one processor adapted to selectively control the retrieval subsystem to retrieve a record in dependence on a compliance with respective set of access rules;

at least one communications port, adapted to communicate the record in an encrypted form requiring for decryption at least one temporary session key generated for conduct of communications during a respective communications session, and a private key of a persistent public key-private key pair, and wherein access of the record is controlled through a wrapper which is adapted to generate a communicated access message through the communications port, and which is communicated to the at least one retrieval system for updating the at least one access log.

153. (New) The database system according to claim 152, wherein each respective set of access rules represents instructions to a trustee operating under an established legal trust, applying the access rules on behalf of a beneficiary in accordance with the legal trust, the respective access rules, and the jurisdictional trust law.

154. (New) A method, comprising the steps of:

storing a set of access rules in a database;

defining a plurality of sets of information content, the sets of information content being subject to associated access rules stored in the database;

transmitting information defining the associated access rules for the respective plurality of sets of information content to a database control system;

automatically, under control of the database control system, retrieving the associated access rules with respect to the associated information content, and implementing the retrieved associated access rules dependent on a context of attempted access of the associated information content;

communicating the associated information in an encrypted form, an access to a decrypted form of the information content being dependent at least a transient session key and a private key of a persistent public key-private key pair; and

accounting for access to the information content and respective context in an access log based on a wrapper associated with the information content.

155. (New) The method according to claim 154, wherein the respective set of access rules comprise instructions to a trustee, defined under a legally enforceable trust agreement establishing a trust granting legal control over access to the record to a trustee subject to jurisdictional law of trusts, on behalf of a beneficiary, the limitations of the trust being enforced under authority of the trustee in accordance with the trust agreement, the respective set of access rules, and the jurisdictional law of trusts.

156. (New) A data security method for controlling access to a plurality of records comprising:

providing a plurality of automated electronic databases, each having a plurality of records and being controlled by a custodian;

identifying the owner and respective custodian of a record in a respective automated electronic database, each record having an associated set of access rules and compensation rules;

determining other records associated with the identified owner;

receiving a request for access;

determining a set of records corresponding to the request for access, comprising records associated with a single owner maintained in respective automated electronic databases controlled by a plurality of custodians, a compliance with respective non-economic access rules for members of the set of records, and a compensation associated with the request for access based on the economic compensation rules;

retrieving members of the set of records, from the automated electronic database, for which the non-economic access rules permit access and the economic compensation rules have been satisfied by providing economic compensation to at least one of (i) the record owner and (ii) at least one custodian; and

updating an access log in dependence on at least one of an access to the records and an attempted access to the records.

157. (New) The method according to claim 156, wherein the respective set of access rules comprise instructions to a trustee, defined under a legally enforceable trust agreement establishing a trust granting legal control over access to the record to a trustee subject to jurisdictional law of trusts, on behalf of a beneficiary, the limitations of the trust being enforced under authority of the trustee in accordance with the trust agreement, the respective set of access rules, and the jurisdictional law of trusts.

158. (New) The method according to claim 156, further comprising:

storing the set of access rules in a database;

transmitting information defining the access rules for the respective plurality of records to a database control system;

automatically, under control of the database control system, retrieving the associated access rules with respect to the determined set of records, and implementing the retrieved associated access rules dependent on a context of attempted access of the associated information content; and

communicating at least one record in an encrypted form, an access to a decrypted form of the information content being dependent at least a transient session key and a private key of a persistent public key-private key pair,

wherein the access log is updated based on a wrapper associated with the information content.

159. (New) The method according to claim 158, wherein the respective set of access rules comprise instructions to a trustee, defined under a legally enforceable trust agreement establishing a trust granting legal control over access to the record to a trustee subject to jurisdictional law of trusts, on behalf of a beneficiary, the limitations of the trust being enforced under authority of the trustee in accordance with the trust agreement, the respective set of access rules, and the jurisdictional law of trusts.